

son ordinateur ou de son smartphone, elle circule sur le réseau des nœuds validateurs qui ne peuvent que l'accepter et exécuter ce qu'elle demande. L'opération est irréversible. Cette irréversibilité n'existe pas pour les virements dans le monde bancaire classique, où les établissements gardent pendant plusieurs jours la possibilité d'annuler un virement. Cette irréversibilité des transactions en cryptomonnaies est intéressante et a été généralisée avec ce qu'on dénomme des contrats intelligents, ou *smart contracts*. Ce sont des programmes qu'on dépose sur la blockchain de certaines cryptomonnaies et qui ont la capacité de détenir des unités monétaires, d'en recevoir et d'en envoyer automatiquement.

La première cryptomonnaie à offrir un langage puissant pour écrire ces *smart contracts* était ethereum (voir « Du bitcoin à ethereum : l'ordinateur-monde », Pour la Science de novembre 2016, pp. 104-109). L'irréversibilité devient pour un *smart contract* l'impossibilité d'en arrêter le fonctionnement, qui est simultané sur chaque nœud validateur. Cela interdit de faire exécuter au programme autre chose que ce qui est prévu. Ces programmes qui, une fois définis, ne peuvent plus être arrêtés ou modifiés parce que leur fonctionnement provient du consensus d'exécution du réseau, constituent une nouveauté informatique extraordinaire. Cet ordinateur mondial, décentralisé, parfaitement fiable fait ce qu'on lui demande de faire sans que personne ne puisse l'interrompre ou le corrompre.

Cela permet par exemple de programmer des jeux d'argent et de pari où l'organisateur ne peut pas refuser de payer et ne peut partir avec la caisse quand il perd trop. Le terme d'applications décentralisées (DApp, en abrégé anglo-saxon) est souvent utilisé pour désigner ces *smart contracts*.

Grâce à ces *smart contracts*, on crée des cryptomonnaies qui ont les mêmes propriétés que celles reposant sur des blockchains spécifiques : elles sont sans autorité centrale et surveillées, indirectement maintenant, par les nœuds validateurs d'un réseau. En clair, grâce aux cryptomonnaies permettant les *smart contracts*, on définit facilement de nouvelles monnaies décentralisées sans avoir à mettre en place un réseau nouveau de nœuds validateurs.

Cette possibilité de disposer de l'équivalent d'une blockchain particulière à moindre coût en s'appuyant par exemple sur la blockchain ethereum a engendré l'apparition rapide de nouvelles cryptomonnaies, dont le nombre a explosé depuis 2016. Des cryptomonnaies liées à certaines entreprises voulant lever des fonds ont été introduites par dizaines. Les unités monétaires de ces cryptomonnaies se nomment des jetons (*tokens*) et ces opérations de

2

LES ICO OU PRÉÉMISSIONS DE JETONS

Une ICO (pour *initial coin offering*, ou « préémission de jetons ») est une méthode de levée de fonds fondée sur une cryptomonnaie liée à l'entreprise qui veut se financer. Les jetons de la cryptomonnaie sont en général créés à l'aide d'un *smart contract* (voir le texte principal). On peut acheter des jetons pendant la phase de démarrage de l'entreprise. Ces jetons sont cotés et échangeables sur les plateformes d'échange de cryptomonnaies. Le plus souvent le bitcoin ou l'ether sert de monnaie intermédiaire : on achète des bitcoins pour ensuite les échanger contre des jetons de l'ICO.

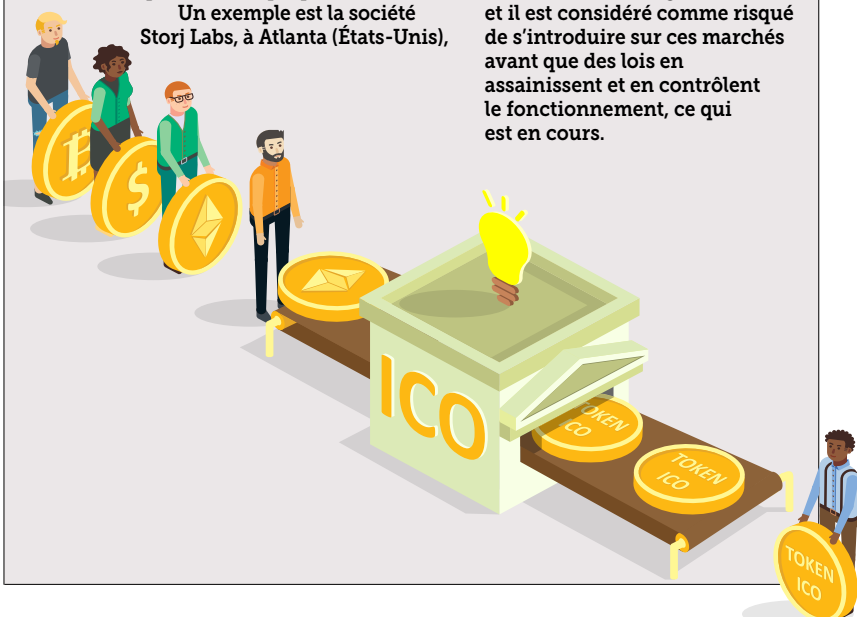
Les jetons de l'ICO donnent des droits particuliers concernant l'entreprise qui les a émis : droits de vote, droits d'usage des services à prix intéressants, etc. Contrairement aux actions mises en circulation lors d'une IPO (*initial public offering*, en français « introduction en Bourse »), les jetons ne représentent pas des parts de l'entreprise. Acheter les jetons d'une ICO revient à prépayer les services qui vont être proposés.

Un exemple est la société Storj Labs, à Atlanta (États-Unis),

qui crée un service de stockage massif décentralisé. Les fichiers informatiques à stocker sont chiffrés et découpés en morceaux. On les copie alors – avec des redondances pour se protéger des accidents – dans la mémoire des ordinateurs acceptant de participer au réseau de stockage. La capacité du réseau dépasse 100 pétaoctets (soit 10^{17} octets), et l'objectif est d'arriver à plusieurs exaoctets (10^{18} octets). Le réseau est déjà composé de 150 000 ordinateurs capables de détenir des morceaux de fichiers confiés à Storj répartis dans 200 pays.

La société Storj Labs a levé début 2017 l'équivalent de 30 millions de dollars via une ICO. Leur jeton, le *storjcoin*, permet d'acheter de l'espace de stockage sur le réseau Storj ; il représente donc un accès privilégié aux services développés. La capitalisation des jetons Storj en février 2019, (victime de la baisse générale des cours de l'année 2018) s'élevait à 18 millions de dollars. Si la société réussit, ses jetons se valoriseront.

Contrairement aux IPO, les ICO sont mal réglementées et il est considéré comme risqué de s'introduire sur ces marchés avant que des lois en assainissent et en contrôlent le fonctionnement, ce qui est en cours.





MONTÉE EN FLÈCHE DES STABLECOINS

3

Puisque la volatilité des cours des monnaies cryptographiques rend impossible leur usage comme « réserve de valeur », ou même comme instrument de paiement, il fallait empêcher cette volatilité.

L'idée la plus simple est d'offrir à tout détenteur d'une unité de la cryptomonnaie la capacité de l'échanger contre un actif précis ayant une valeur qui, par définition, sera considérée comme fixe, par exemple un dollar. La possibilité de cet échange rend absurde d'attribuer à l'unité en question une valeur moindre. Si, en plus, à chaque fois que quelqu'un veut disposer d'une unité de cette cryptomonnaie, on lui donne la possibilité de l'acquérir à ce coût fixé à l'avance, le cours de la cryptomonnaie ne pourra pas monter. C'est l'idée des *stablecoins*, ou « jetons stables ». Ces *stablecoins*, comme les cryptomonnaies, reposent directement ou indirectement sur une blockchain, ce qui assure la nature décentralisée et irréversible des transactions et du fonctionnement des comptes, et permet l'anonymat. Cependant, il faut que celui qui propose ces échanges 1 contre 1 (par exemple avec le dollar) soit crédible. Il faut pour cela qu'il organise un système d'audit indépendant attestant qu'il met en réserve la contrepartie des unités qu'il fait circuler. Cette contrepartie gardée en réserve par un acteur déterminé constitue un aspect centralisé de la cryptomonnaie. Ceux qui sont attachés à l'idée d'une décentralisation complète considèrent cela regrettable. Insistons sur le fait que la gestion des comptes est décentralisée et qu'un tel *stablecoin* n'est donc pas centralisé comme l'est une monnaie d'État : on gagne donc bien quelque chose, en plus

de la fluidité et de la stabilité du cours, avec les *stablecoins*.

Les principales *stablecoins*, avec leur capitalisation et leur cours en dollars (\$), sont :

USD Tether : 2 032 525 000 \$	1 USDT = 1,00 \$
USD coin : 247 268 000 \$	1 USDC = 1,00 \$
True USD : 200 244 000 \$	1 TUSD = 1,01 \$
Nano : 135 067 000 \$	1 Nano = 1,01 \$
Paxos Standard : 118 657 000 \$	1 PAX = 1,00 \$
Dai : 87 789 000 \$	1 DAI = 0,99 \$

Le *stablecoin* dai fonctionne selon un mécanisme différent de celui décrit plus haut. Ce mécanisme est, lui, totalement décentralisé et s'appuie sur une surcontrepartie en cryptomonnaie (par exemple de 1,5 dollar de cryptomonnaie pour 1 dollar de *stablecoin*) qui permet de garantir la stabilité... à la condition que les variations de cours de la cryptomonnaie utilisée pour adosser le *stablecoin* ne soient pas trop brusques. De nouveaux modèles de *stablecoins* totalement décentralisés sont en cours d'expérimentation.

Le succès des *stablecoins* en 2018 a été remarquable. De 30 projets de *stablecoins* (dont 9 en fonctionnement) au début de 2018, on est passé début 2019 à plus de 160 projets (dont 28 fonctionnent). La capitalisation boursière totale de ces *stablecoins* a doublé durant la même période, passant d'environ 1,5 milliard à presque 3 milliards de dollars. Notons aussi que les *stablecoins* pourraient être plus facilement acceptés par les autorités monétaires : par exemple, les régulateurs financiers de l'État du Texas, aux États-Unis, envisagent de donner aux *stablecoins* un statut de monnaie au même titre que l'euro ou le yen.

➤ levée de fonds se nomment ICO, pour *initial coin offering*, par analogie avec IPO, pour *initial public offering* (« introduction en Bourse »).

Plusieurs milliards de dollars ont pu ainsi être trouvés pour le financement de start-up, qui travaillent en général dans le domaine des cryptomonnaies ou des blockchains. Cependant, contrairement aux IPO, qui sont très réglementées, les ICO ne le sont pas assez et elles ont été utilisées pour organiser diverses escroqueries. Elles sont interdites en Chine et les autorités financières de nombreux pays invitent à s'en méfier. L'émission et la manipulation de ces jetons sont fiables, mais pas ce qu'ils représentent, car les entreprises financées par l'achat de ces jetons sont parfois des coquilles vides. En France, l'Autorité des marchés financiers (AMF) va attribuer des labels pour que les acheteurs intéressés par les ICO puissent y voir clair.

Précisons que d'autres cryptomonnaies ont suivi ethereum en offrant la possibilité sur leur blockchain de déposer des *smart contracts*. Le réseau des bitcoins ne permet pas l'écriture de *smart contracts* qui seraient déposés sur sa blockchain, mais une blockchain connectée à celle des bitcoins dénommée *rootstock* le permet. Les cryptomonnaies ripple, EOS, NEO, cardano autorisent aussi la création de *smart contracts*.

DES CRYPTOMONNAIES SANS PREUVE DE TRAVAIL

Les monnaies fonctionnant avec des « preuves de travail » pour récompenser ceux qui acceptent d'être des nœuds validateurs du réseau et contribuent à ce qu'il fonctionne ont deux graves défauts. Le premier est que leur fonctionnement et leur sécurité exigent une dépense continue et importante d'électricité. L'article publié en février 2018 dans cette rubrique « La folie électrique du bitcoin » (pp. 80-85) détaillait ce problème. Une mise à jour des chiffres de cet article donne comme conclusion qu'aujourd'hui la dépense annuelle électrique du réseau des bitcoins est supérieure à 40 térawattheures (TWh) d'électricité. C'est équivalent à ce que produisent en un an cinq réacteurs nucléaires ! Par comparaison, les *datacenters* de Google dépensent moins de 6 TWh par an.

Le second grave défaut des cryptomonnaies utilisant des preuves de travail est que cela crée pour elles un handicap concurrentiel face aux monnaies cryptographiques n'utilisant pas les preuves de travail.

En effet, le fonctionnement d'un réseau de cryptomonnaies a un certain coût, qui d'une façon ou d'une autre doit être payé par les utilisateurs. Les émissions nouvelles d'unités monétaires créent une pression d'inflation et font perdre de la valeur aux unités déjà émises (ce qui est une façon indirecte de faire payer